

ALL EMPLOYEE BULLETIN #01-09

ACCESSING AND HANDLING NON-PUBLIC MATERIAL

I. INTRODUCTION

Employees (including contractor employees) may encounter non-public material, the disclosure of which may harm the Commission's deliberative process or cause competitive harm or other business injury to entities submitting such material to the Commission. Non-public material includes material under seal, material submitted with a request for privileged treatment, and internal or interagency documents that fall within an exemption to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552. The purpose of this bulletin is to remind all employees of their continuing responsibilities for safeguarding non-public material submitted to the Commission, and to set forth Commission procedures for accessing such material. To the extent that any information in this bulletin conflicts with FERC AD 4-20 or the associated procedural manuals, the information in this bulletin supersedes those documents. This bulletin does not address: (1) internal non-public material, (2) investigative material, or (3) additional restrictions that may apply to the release of information, such as those contained in the Privacy Act, the Trade Secrets Act, and the Computer Security Act. Information regarding access and handling of internally-generated non-public material and investigative material will be addressed in the near future.

All employees are responsible for ensuring the protection of non-public material. Employee work products containing protected or privileged material must be marked as such and treated accordingly. Any employee who notices that non-public material is being treated in a manner inconsistent with this bulletin must notify their supervisor immediately.

II. DEFINITIONS

- A. **Protected or sealed material** – material filed subject to a protective order issued by the Commission or an Administrative Law Judge. The filer submits only one copy of this material; it is submitted in a sealed envelope. This material is not scanned into the Records and Information Management System ("RIMS").
- B. **Privileged material** – material filed under 18 C.F.R. § 388.112 with a request for privileged treatment by claiming that some or all of the material contained in the document is exempt from mandatory public disclosure under FOIA. Generally these materials will involve trade secrets, or commercial or financial material exempt from disclosure under FOIA exemption (b)(4). These documents are kept in the Commission's non-public files. This material is scanned into RIMS.

- C. **Internal non-public material** – internal or interagency material that falls within an exemption under FOIA, including but not limited to material related to internal administrative rules and practices of the agency, and material subject to the deliberative process privilege, the attorney-work-product privilege, or the attorney-client privilege. Examples of internal non-public material include: drafts, internal memoranda, notes from deliberative meetings, Privacy Act records, and security procedures. These materials are not, of course, scanned into RIMS. This bulletin does not cover internal non-public materials.
- D. **Investigative material** – non-public material collected in the course of an investigation under 18 C.F.R. Part 1b, "Rules relating to investigations." This bulletin does not cover investigative material.

III. **ACCESS AND HANDLING OF NON-PUBLIC MATERIAL**

A. **PROTECTED/SEALED MATERIAL**

This section covers access and handling of protected material by staff who have not signed a non-disclosure certificate pursuant to a protective order. (Staff who signs a non-disclosure certificate is bound by the terms and restrictions of the certificate and the associated protective order.)

1. **Access to Protected/Sealed Material**

Requests for access are presented to the Records Maintenance Center ("RMC") Control Desk, along with the employee's identification badge, and authorization by the office director or designee. Office director authorization normally will be limited to those involved in the case. Each employee will be required to sign a confidentiality agreement prior to receiving protected materials.

2. **Handling Protected/Sealed Material**

Before receiving protected material, staff must agree in writing to:

- Not make any copies of the material, fax the material, or otherwise transmit the material.

- Not show the material to or discuss the contents of the material with anyone unless that person has a need to know the information in order to perform his or her official duties. If there is a question regarding another employee's need for the information, the employee with the protected material should seek authorization by his or her office director or designee prior to sharing the material with the other employee.
- Safeguard the material until the employee returns it to the RMC, securing it in a locked room or locked cabinet whenever it is out of the employee's sight.
- Keep the material on Commission premises unless the office director or designee gives written authorization to take the material off the premises.
- Return protected material to the RMC Control Desk as soon as it is no longer needed. Material will be returned within 30 days unless the office director or designee authorizes an extension. Upon return, an employee will certify that all material received has been returned to the RMC.

RMC staff will contact employees every 30 days to verify that they have a continuing need and authorization for the material.

B. MATERIAL SUBMITTED WITH A REQUEST FOR PRIVILEGED TREATMENT UNDER 18 C.F.R. § 388.112

1. Access to Privileged Material

Office directors will determine which employees will be granted access to the RIMS non-public materials. **Any staff member granted such access may only access non-public material if assigned to the matter and if the material is needed to perform official duties.** The Chief Information Officer will conduct periodic audits of staff access to non-public material, and employees may be required to explain the reason(s) they accessed particular non-public material.

Employees who request non-public material from the RIMS Help Desk or through the RMC Control Desk must provide an employee identification badge, and present a form signed by the employee and the office director or designee certifying that the material is needed to perform official duties related to that proceeding.

2. Handling Privileged Material

The following special handling instructions are required to safeguard privileged materials:

- An employee working on a case where privileged material has been filed may use the original from the RMC Control Desk, or may obtain one copy from RIMS or the RIMS Help Desk. An employee will not make any additional copies of privileged materials, and may not fax, e-mail or otherwise transmit privileged materials.
- The employee may not share or discuss privileged material with anyone outside of the Commission.
- The employee may not show or discuss privileged material with anyone unless that person has a need to know the information in order to perform his or her official duties. If there is a question regarding another employee's need for the information, the employee with the privileged material should seek authorization by his or her office director or designee prior to sharing the material with the other employee.
- Any employee who has been granted written access by the office director or designee may obtain one copy from RIMS, the RIMS Help Desk or the RMC.
- The employee must safeguard privileged material by securing it in a locked room or locked cabinet whenever it is out of the employee's sight.
- The employee may not remove the material from Commission premises without written approval of the office director or designee.
- The employee must dispose of any copy of privileged material by shredding it or placing it in a burn bag once it is no longer needed. If the material is the original, it should be returned to the RMC Control Desk.

IV. MISHANDLING OR MISUSE OF NON-PUBLIC INFORMATION

Employees who mishandle or misuse non-public materials in any way are subject to disciplinary action, up to and including removal from Federal service. Further, criminal penalties may apply for improper disclosure of non-public material.

V. FEDERAL NOTICE REQUIREMENT

These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employees' obligations, rights, or liabilities created by Executive Order No. 12958; section 7211 of title 5, U.S.C.; section 1034 of title 10, U.S.C., as amended by the Military Whistleblower Protection Act; section 2302(b)(8) of title 5, U.S.C., as amended by the Whistleblower Protection Act; the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 *et seq.*); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952 of title 18, U.S.C., and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this bulletin and are controlling.

VI. ASSISTANCE

Questions concerning this bulletin should be forwarded to OGC. General and Administrative Law, 208-0457. Email inquiries may be sent to Carol Johnson.